Non-Proprietary FIPS 140-2 Security Policy: Key Variable Loader (KVL) 4000 PIKE2

Document Version: 1.1

Date: December 22, 2020

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Motorola Solutions Key Variable Loader (KVL) 4000 PIKE2 module, hereafter denoted the Module. The KVL 4000 is a portable key distribution device that consists of a Personal Digital Assistant (PDA) and Security Adapter (SA) that connects to the PDA. The PIKE2 IC is embedded in the SA; PIKE2 IC is a single-chip cryptographic module to meet FIPS 140-2 Level 3 Physical Security requirements as defined by FIPS 140-2. Encryption keys can be loaded into the KVL 4000 manually through its keypad interface, randomly generated internally by the SA, or transferred from a key management facility through its RS-232 interface. These keys can then be distributed to various secure communications equipment such as mobile and portable radios, base stations, zone controllers, data controllers, and other fixed network devices.

Table 1 – Cryptographic Module Configuration

Module	HW P/N and Version	Base FW Version
Key Variable Loader (KVL) 4000 PIKE2	51009397004	R02.07.30

The Module supports the following FIPS Approved algorithms which may be installed separately from the Module firmware using the Program Update service. While the installation of AES may be done separately, for the purposes of this validation the module includes this firmware.

Table 2 – Approved Mode Drop-in Algorithms

Algorithm	Algorithm FW Version	Base FW Version	Cert. #
AES128	R01.01.00	R02.07.30	1491
AES256	R01.01.00	R02.07.30	1492

Table 3 – Non-Approved Mode Drop-in Algorithms

Algorithm	Algorithm FW Version	Base FW Version
ADP	R01.00.00	R02.07.30
CFX-256	R01.00.00	R02.07.30
DES (ECB, OFB and CBC modes)	R01.00.00	R02.07.30
DES-XL	R01.00.00	R02.07.30
DVI-XL	R01.00.00	R02.07.30
DVP-XL	R01.00.00	R02.07.30
Localized Capable (Custom DIA)	R01.00.00	R02.07.30

The Module is intended for use by the markets that require FIPS 140-2 validated overall security level 2.

The Module was previously FIPS 140-2 validated with the following FW versions.

Table 4 – Historical FIPS 140-2 Validation Status

CMVP Cert#	FW Version
2251	R02.03.07, R02.05.03, R02.05.05, and R02.05.08
2250	R02.03.07, R02.05.03, R02.05.05, and R02.05.08

The FIPS 140-2 security levels for the Module are as follows:

Table 5 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall	2

1.1 Module Description and Cryptographic Boundary

The KVL 4000 Key Variable Loader (KVL) production diagram is shown in the Figure 1 below. The KVL 4000 PIKE2 IC in the Security Adapter provides data security services required by the KVL 4000 key loader.

Figure 1: KVL 4000 Key Variable Loader (KVL)

The Crypto Boundary is drawn around the KVL PIKE2 IC as shown in Figure 2 below.

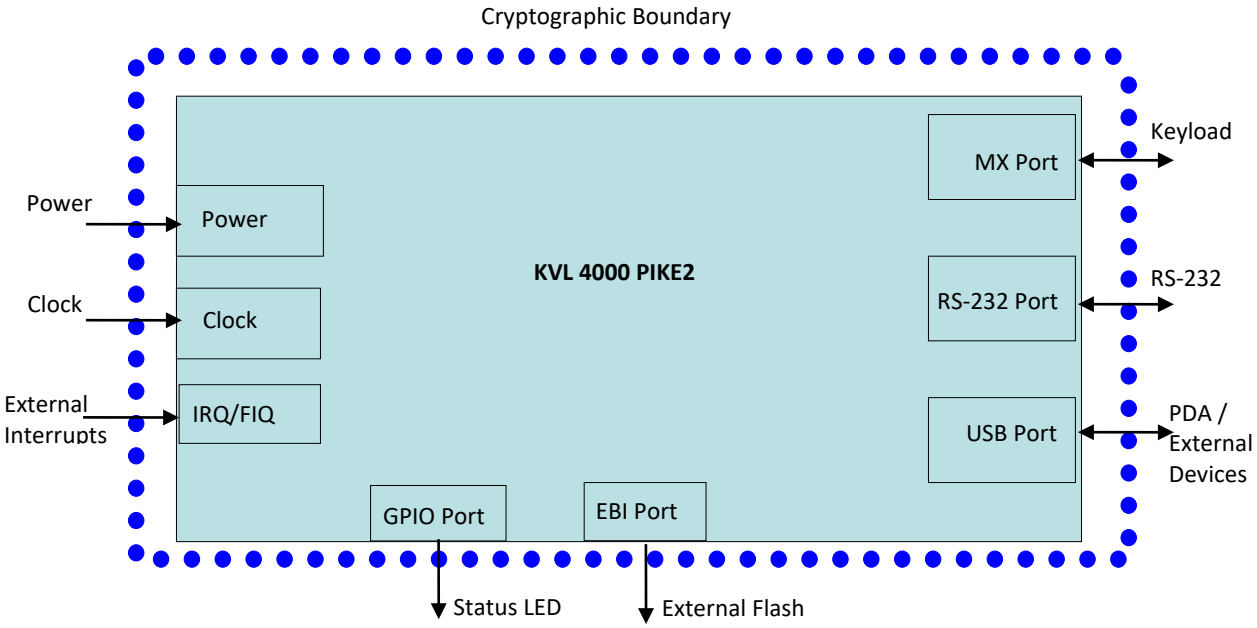

Figure 2: KVL 4000 PIKE2 Cryptographic Boundary

The Module's ports and associated FIPS defined logical interface categories are listed in Table 6.

Table 6 – Ports and Interfaces

Port	Description	Logical Interface Type
Power	This interface powers all circuitry. This interface does not support input/output of CSP's.	Power Input
Universal Serial Bus (USB) Interface	This is the interface to the PDA host software, and to external devices. CSPs exchanged over this interface are always encrypted.	Data Input Data Output Control Input Status Output
Keyload (MX) Interface	This is the interface to external devices. CSPs exchanged over this interface are either encrypted or plaintext when operating in FIPS approved mode.	Data Input Data Output
RS-232 Interface	Provides an interface for factory programming and execution of RS-232 shell commands. CSPs exchanged over this interface are always encrypted when operating in FIPS approved mode.	Data Input Data Output Status Output

Port	Description	Logical Interface Type
EBI Interface	This is the interface to the external flash memory on the KVL 4000 Security Adapter. CSPs exchanged over this interface are always encrypted when operating in FIPS approved mode.	Data Input Data Output
GPIO	This is the interface to control the LED of the KVL4000. The output turns flashing amber during self-tests and momentary solid green after self-tests are completed successfully. The LED output turns solid red upon entering a critical error state.	Status Output
IRQ/FIQ	External interrupts.	Control Input
Clock	Clock Input.	Control Input

2 Modes of Operation

The Module can be configured to operate in a FIPS 140-2 Approved mode of operation and a non-Approved mode of operation. The KVL 4000 will be configured to operate in a FIPS 140-2 Approved mode of operation by following the steps in Section 2.1. Disabling FIPS-140-2 in the settings menu of the KVL Host application graphical user interface in the settings menu will transition between FIPS 140-2 Approved and non-Approved modes. An operator must change the value of CSPs via the Program Update service as mentioned in section 3.1; all other CSPs are automatically zeroized by the Module when switching FIPS modes. At any given time, the FIPS Status service can be used to determine whether the module is operating in a FIPS approved or in a non-FIPS Approved mode.

The Version Query service can also be used to verify the firmware version matches an approved version listed on NIST's website: https://csrc.nist.gov/groups/STM/cmvp/validation.html

2.1 Approved Mode Configuration

Documented below are the actions and configuration settings required to enable FIPS 140-2 approved mode.

- Enable User and Crypto-Officer passwords.
- Enable FIPS 140-2 in the settings menu of the PDA graphical user interface.
- Additionally, the Module supports "drop-in algorithms" via the Program Update service. Drop-in algorithms may be added or removed from the Module independent of the base FW. In order to remain in the Approved mode, only Approved algorithms may be loaded into the Module; in particular AES-128 (Cert. #1491) and/or AES-256 (Cert. #1492).

3 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved-but-Allowed cryptographic functions listed in the tables below.

Table 7 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
1491	AES [197]	ECB [38A]	Key Sizes: 128	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 128	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 128	Encrypt, Decrypt
1492	AES [197]	ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
		CFB8 [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
C1297	AES [197]	CFB8 [38A]	Key Sizes: 256	Encrypt, Decrypt
		ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
1491	AES [197]	KW [38F]	Forward Key Sizes: 128	Authenticated Encrypt, Authenticated Decrypt
5451	AES [197]	KW [38F]	Forward Key Sizes: 256	Authenticated Encrypt, Authenticated Decrypt
VA	CKG [IG D.12]	[133] Section 7.1 Direct symmetric key generation using unmodified DRBG output		Key Generation
C1298	DRBG [90A]	CTR	AES-256	Deterministic Random Bit Generation
183	ECDSA [186]		P-384 SHA(384)	SigVer
N/A	KTS [38F]	KW	AES Cert. #1491	Key establishment methodology provides 128 bits of encryption strength
N/A	KTS [38F]	KW	AES Cert. #5451	Key establishment methodology provides 256 bits of encryption strength
1345	SHS [180]	SHA-256 SHA-384		Message Digest Generation, Password Obfuscation

Table 8 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
AES Key Unwrap	[IG G.9] AES-OFB (Cert. #1491) key unwrapping for use in key transport; provides 128 bits of encryption strength.
AES Key Unwrap	[IG G.9] AES-OFB (Cert. #1492) key unwrapping for use in key transport; provides 256 bits of encryption strength.

Algorithm	Description
AES Key Wrap (no security claimed)	[IG 1.23] AES-OFB key wrapping for use in obfuscation of keys transported in plaintext.
AES MAC [IG G.13]	[IG G.13] AES MAC for Project 25 APCO OTAR (AES Cert. #1492)
NDRNG	[IG G.13] Non-Deterministic RNG used for seeding the DRBG. Each 128-bit block output from the entropy source is assessed to contain 42.957 bits of min entropy.

Non-Approved Cryptographic Functions for use in non-FIPS mode only:

- ADP
- CFX-256
- DES-XL
- DES (ECB, OFB, and CBC modes)
- DVI-XL
- DVP-XL
- Localized Capable (Custom DIA)

Note that all of the above are “drop-in” algorithms.

3.1 Critical Security Parameters

All CSPs used by the Module are described in this section. Usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4. It should be noted that Keys/CSPs stored in non-volatile memory/storage are normally preserved during a Program Update. However, all keys/CSPs are zeroized during a Program Update if the Module’s FIPS status changes, post-upgrade (this indicates that a non-FIPS compliant Drop-in algorithm has been loaded onto the Module)

Table 9 – Critical Security Parameters (CSPs)

CSP	Description / Usage
DRBG Entropy Input	A 2048-bit of entropy used in seeding of the CTR_DRBG during DRBG instantiation at power-up. Stored plaintext in the volatile memory, and zeroized by power cycling. It is not entered into or output from the module.
DRBG Internal State (V and Key)	Internal state of SP800-90A CTR_DRBG (V and Key). Stored plaintext in the volatile memory, and zeroize by power cycling. It is not entered into or output from the module, generated through SP800-90A CTR_DRBG state modification.
Black Keyloading Key (BKK)	A 256-bit AES key used for obfuscating keys output over the MX and RS-232 ports. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The BKK is entered using the Program Update service and is not output from the module.

CSP	Description / Usage
FIPS Cipher Key (FCK)	A 256-bit AES key used for obfuscating and decrypting keys and passwords entered into the module over the USB port. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The FCK is entered using the Program Update service and is not output from the module.
Image Decryption Key (IDK)	A 256-bit AES key used to decrypt downloaded images. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The IDK is entered using the Program Update service and is not output from the module.
KPK Encryption Key (KPKEK)	A 256-bit AES key used to encrypt the KPK. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The KPKEK is entered using the Program Update service and is not output from the module.
Key Protection Key (KPK)	A 256-bit AES key used to encrypt TEKs and KEKs output over the EBI and USB ports. The KPK is generated internally by the SP800-90A CTR DRBG and is not output from the module. Stored in plaintext in volatile memory and encrypted with the KPKEK in non-volatile memory. Zeroized by power cycle for volatile memory.
Key Encryption Keys (KEKs)	A 256-bit AES key used for encryption/obfuscation of KEKs/TEKs in the Store and Forward, and Transfer Key Variable services. Stored in plaintext in the volatile memory and zeroized by power cycle. Entry: USB interface from Host Application - AES256 OFB encrypted by the FCK. Store and Forward service via RS-232 interface - AES MAC (OTAR) encrypted by the other KEK. Key Sharing Service via MX Port - Plaintext (clear) Output: (plaintext) MX Port - AES256 OFB obfuscated [IG1.23] by the BKK. USB port to PDA Host Application - AES256 OFB obfuscated by the FCK. USB or RS-232 ports to external device (for Transfer key variable service) - AES256 OFB obfuscated by other KEK. Key Sharing Services via MX Port - Plaintext (clear).
Traffic Encryption Keys (TEKs)	128/256-bit AES Key used for enabling secure communication in target devices. Stored in plaintext in the volatile memory and zeroized by power cycle. Entry: USB interface from Host Application - AES256 OFB encrypted by the FCK. Store and Forward service via RS-232 Port - AES MAC (OTAR) encrypted by the KEK. Key Sharing Service via MX Port - Plaintext (clear) Output: (plaintext) MX Port - AES256 OFB obfuscated [IG1.23] by the BKK. USB port to PDA Host Application - AES256 OFB obfuscated [IG1.23] by the FCK. USB or RS-232 ports to external device (for Transfer key variable service) - AES256 OFB obfuscated by the BKK. Key file export service over USB interface: AES256 OFB obfuscated [IG1.23] by the KEK. Key Sharing Services via MX Port - Plaintext (clear).
User Password	A 30-character ASCII password entered encrypted by the FCK and used to authenticate the User role. After decryption the plaintext password is not stored but temporarily exists in volatile memory. The SHA-256 hash of the decrypted password is compared with the hash value stored in non-volatile memory during password validation. The password is not output from the module, and zeroized by power cycle.

CSP	Description / Usage
Crypto-Officer Password	A 30-character ASCII password entered encrypted on the FCK and used to authenticate the Crypto-Officer role. After decryption the plaintext password is not stored but temporarily exists in volatile memory. The SHA-256 hash of the decrypted password is compared with the hash value stored in non-volatile memory during password validation. The password is not output from the module, and zeroized by power cycle.

3.2 Public Keys

Table 10 – Public Keys

Key	Description / Usage
ECDSA Public Programmed Signature Key	A 384-bit ECDSA key used to validate the signature of the firmware image being programmed before it is allowed to be executed and is also used for authentication of the Crypto-Officer role. Loaded during manufacturing, and not output from the module.

4 Roles, Authentication and Services

4.1 Assumption of Roles

The KVL 4000 PIKE2 supports a User and a Crypto-Officer role. Both Crypto-Officer and User role are authenticated by 30 ASCII printable characters in length.

Table 11 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer Role over USB interface	Identity-based	30 character ASCII Password
User	User Role over USB interface	Identity-based	30 character ASCII password

4.2 Authentication Methods

Password Authentication

Since the password length is 30 ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in 95^{30} which is less than 1 in 1,000,000.

The Module limits the number of consecutive failed authentication attempts to a configurable number (Minimum 3, maximum 255). The worst-case probability of a successful random attempt within a one-minute period is $255/95^{30}$, which is less than 1 in 100,000.

The Module takes approximately 167ms to authenticate CO/User logging message over USB interface which translates to 359 attempts per minute. As 255 is the maximum attempts allowed, the worst-case probability of a successful random attempt within a one-minute period is $255/95^{30}$, which is less than 1 in 100,000.

Table 12 – Authentication Description

Authentication Method	Probability	Probability over a One-Minute Period
Password	$1/95^{30}$	$1/95^{30}$ or $255/95^{30}$, depending on configuration

4.3 Services

All services implemented by the Module are listed in the tables below. Note that all services listed in Table 13 and Table 14 below are available in both the FIPS Approved and non-Approved mode. The only distinguishing factor between Approved and non-Approved services is whether non-Approved algorithms/ key establishment schemes are available.

Table 13 – Authenticated Services

Service	Description	CO	User
Program Update	Update the module software. Software upgrades are authenticated using a digital signature. The Public Signature Validation Key (a 384-bit public programmed signature key) is used to validate the signature of the firmware image being loaded before it is allowed to be executed. To maintain validation, only validated software should be loaded. Loading non-validated software will invalidate the modules validation.	X	
Validate Crypto-Officer Password	Validate the current Crypto-Officer password used to identify and authenticate the Crypto-Officer role via the USB interface.	X	
Change Crypto-Officer Password	Modify the current password used to identify and authenticate the CO Role via USB interface.	X	
Validate User Password	Validate the current User password used to identify and authenticate the User role via the USB interface.		X
Change User Password	Modify the current password used to identify and authenticate the User Role via USB interface.	X	X
Configure KVL	Set configuration parameters used in Store and Forward protocols and other module-specific parameters over the USB interface.	X	X
Version and Algorithm List Query	Provides module firmware version number and list of algorithms over the USB interface.	X	X
Logout	Logs out the operator.	X	X

Service	Description	CO	User
Transfer Key Variable	Transfer key variables (KEKs, TEKs) to the target devices over the Keyload (MX), USB and RS-232 interfaces.	X	X
Receive Key Variable	Receive key variables (KEKs, TEKs) from the USB, Keyload (MX), and RS-232 interfaces.	X	X
Generate Key Variable	Auto-generate Keys (KEKs, TEKs) and KPK within the module.	X	X
Delete Key Variable	Delete Keys (KEKs, TEKs) managed by the module.	X	X
Edit Key Variable	Edit Keys (KEKs, TEKs) managed by the module.	X	X
Key Check	Validate the correctness of a Key based on algorithm properties.	X	X
Zeroize Keys	Zeroize Keys (KEKs, TEKs) in the KVL and target devices over the Keyload (MX) and RS-232 interfaces.	X	X
Encrypt	Encrypt plaintext data to be transferred over the USB, Keyload (MX), RS-232, and EBI interfaces.	X	X
Decrypt	Decrypt ciphertext data received over the USB, Keyload (MX), RS-232, EBI interfaces.	X	X
Store and Forward (SAF)	Imports Keys from KMF into the Module, store the Keys internally, then forward to target device attached to the KVL.	X	X
Key File Export	Export TEKs/KEKs into an encrypted key file over USB interface.	X	X
Key Sharing	Combination of receive and Transfer Key Variable service. Transport keys (TEKs/KEKs) between two KVLs.	X	X
Reset	Reset the databases and module parameters to system defaults via a command over the USB interface.	X	X

Table 14 – Unauthenticated Services

Service	Description
Diagnostics	Read logs, run LED test, test external flash erase and write, and other non-security relevant status information over the RS-232 interface.
Perform Self-Tests	Performs module self-tests comprised of cryptographic algorithms test and firmware test. Initiated by a transition from power off state to power on state.
FIPS Status	Provides current FIPS status about whether the module is operating in FIPS approved mode, or in a non-Approved mode of operation. Available without a role.

Table 15 defines the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- C = Check CSP: Check status of the CSP (i.e. existence, size, format, etc.).
- D = Decrypt: Decrypts entered key using other KEK during CSP entry over the Ethernet interface or using the KVL-BKK during CSP entry over the KVL interface. In the case of the Program Update service, decryption will occur using the IDK.
- E = Encrypt: Encrypts key prior to output over the Ethernet interface using a KEK.
- G = Generate CSP: Generates key or establishes over KAS.
- S = Store CSP: Stores CSP in volatile or non-volatile memory.
- U = Use CSP: Uses key internally for encryption/decryption services.
- Z = Zeroize: The service zeroizes the CSP.
- - = No access: the service does not access the CSP.

Table 15 – Security Parameters Access by Service

Service	CSPs and Public Keys											
	DRBG Entropy Input	DRBG Internal state (V and Key)	BKK	FCK	KPKEK	IDK	KEKs	KPK	TEKs	Crypto-Officer Password	User Password	ECDSA Public Programmed Signature Key
Program Update	-	-	D,Z,S	D,Z,S	D,Z,S	U,Z,S	Z	Z	Z	Z	Z	U
Validate Crypto-Officer Password	-	-	-	-	-	-	-	D,G,S	-	D,U,Z	-	-
Change Crypto-Officer Password	-	-	-	-	-	-	-	-	-	D,U,Z,S	-	-
Validate User Password	-	-	-	-	-	-	-	D,G,S	-	-	D,U,Z	-
Change User Password	-	-	-	-	-	-	-	-	-	D,U,Z,S	-	-
Configure KVL	-	-	-	-	-	-	-	-	C,D,E,S,U,Z	C,D,E,S,U,Z	C,D,E,S,U,Z	-
Version and Algorithm List Query	-	-	-	-	-	-	-	-	-	-	-	-
Logout	-	-	-	-	-	-	-	-	-	-	-	-
Transfer Key Variable	-	-	U	-	-	-	U	-	D,E,U	-	-	-
Receive Key Variable	-	-	-	-	-	-	U	-	D,E,S,U	-	-	-
Generate Key Variable	-	U	-	-	-	-	-	-	E,G,S	-	-	-

Service	CSPs and Public Keys											
	DRBG Entropy Input	DRBG Internal state (V and Key)	BKK	FCK	KPKEK	IDK	KEKs	KPK	TEKs	Crypto-Officer Password	User Password	ECDSA Public Programmed Signature Key
Delete Key Variable	–	–	–	–	–	–	Z	–	Z	–	–	–
Edit Key Variable	–	–	–	–	–	–	D,S	–	D,S	–	–	–
Key Check	–	–	–	–	–	–	C	–	C	–	–	–
Zeroize Keys (in target devices)	–	–	–	–	–	–	–	–	–	–	–	–
Encrypt	–	–	U	U	U	–	U	U	U	–	–	–
Decrypt	–	–	U	U	U	U	U	U	U	–	–	–
Store and Forward (SAF)	–	–	–	–	–	–	U	–	D,E,S,U.Z	–	–	–
Key Sharing	–	–	–	–	–	–	C,S	–	C,S	–	–	–
Key File Export	–	–	U	–	–	–	–	U	D,E,U	–	–	–
Reset	G,U,Z	G,U,Z	–	–	–	–	Z	–	Z	Z	Z	–
Diagnostics	–	–	–	–	–	–	–	–	–	–	–	–
Perform Self-Tests	–	–	–	–	–	–	–	–	–	–	–	–
FIPS Status	–	–	–	–	–	–	–	–	–	–	–	–

5 Self-tests

The Module performs self-tests to ensure the proper operation of the Module. Per FIPS 140-2 these are categorized as either power-up self-tests or conditional self-tests. Power-up self-tests are available on demand by power cycling the Module.

All algorithm Known Answer Tests (KATs) must be completed successfully prior to any other use of cryptographic functionality by the Module. The Module outputs a status indicator via the LED Output interface (GPIO port) to indicate all self-tests passed or when critical error state is entered due to a failed self-test. LED status solid green means power-up self-tests passed, flashing yellow means self-tests is in progress, solid red means the Module is in critical error state due to power-up self-tests failure or critical error condition. The critical error state may be exited by powering the Module off then on.

The Module performs the following algorithm KATs on power-up. The AES KATS are inclusive of the drop-in algorithms.

- Firmware Integrity: A digital signature is generated over the base firmware and all Drop-in algorithms code when it is built using SHA-384 and ECDSA P-384 and is stored with the code upon download into the Module. When the Module is powered up the digital signature is verified. If the digital signature matches, then the test passes, otherwise it fails.
- AES-128 encrypt and decrypt KATs for ECB, OFB, and CBC modes (Cert. #1491).
- AES-256 encrypt and decrypt KATs for CBC, CFB-8, ECB and OFB modes (Cert. #1492).
- AES-256 encrypt and decrypt KATs for CFB-8, ECB and OFB modes (Cert. #C1297).
- AES-128 and AES-256 KW KAT.
- SHA-256 KAT.
- CTR DRBG KAT.

The Module performs the following critical functions tests as indicated.

- Random Number Generator entropy test. This test runs two RNG statistical tests: a FIPS monobit test, and a FIPS “runs” test as defined in SP 800-22r1a.
- The Module performs a read/write test of the internal RAM at each power up.

The Module performs the following conditional self-tests as indicated.

- Continuous Random Number Generator test: The continuous random number generator test is performed on the NDRNG and DRBG supported by the Module. An initial value is generated and stored upon power up. This value is not used for anything other than to initialize comparison data. A successive call to NDRNG/DRBG generates a new set of data, which is compared to the comparison data. If a match is detected, this test fails; otherwise the new data is stored as the comparison data and returned to the caller. This testing is done for each 4 byte NDRNG/16 byte DRBG data block, generated by the DRBG. The Module enters the critical error State if this test fails.
- DRBG Health tests.
- Firmware load test: a digital signature is generated over the code when it is built using SHA-384 and ECDSA P-384. Upon download into the Module, the digital signature is verified. If the digital signature matches, then the test passes, otherwise it fails.

6 Physical Security Policy

The KVL 4000 PIKE2 is a production grade, single-chip cryptographic module as defined by FIPS 140-2 and is designed to meet Level 3 physical security requirements. The KVL 4000 PIKE2 is covered with a hard opaque epoxy coating that provides evidence of attempts to tamper with the module. The KVL 4000 PIKE2 does not contain any doors, removable covers, or ventilation holes or slits. No maintenance access interface is available. No special procedures are required to maintain physical security of the module while delivering to operators. Physical Security Testing was performed at ambient temperature.

7 Operational Environment

The Module has a non-modifiable operational environment under the FIPS 140-2 definitions. The Module includes Program Update service to support necessary updates. Firmware versions validated through the

FIPS 140-2 CMVP will be explicitly identified on a validation certificate. If firmware that is not identified in this Security Policy is loaded into the Module, the Module will be in a non-Approved mode.

8 Mitigation of Other Attacks Policy

The Module is not designed to mitigate any specific attacks outside of those required by FIPS 140-2.

9 Security Rules and Guidance

This section documents the security rules for the secure operation of the Module to implement the security requirements of FIPS 140-2.

9.1 Invariant Rules

1. An operator does not have access to any cryptographic services prior to assuming an authorized role.
2. Power up self-tests do not require any operator action.
3. Data output is inhibited during key generation, self-tests, zeroization, and while in critical error states.
4. The Module does not perform any cryptographic functions while in critical error state.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
6. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
7. The Module provides a means to ensure that a key entered into or stored within the module is associated with the correct entities to which the key is assigned. Each TEK, KEK in the Module is entered and stored with the following information:
    - Key Identifier – 16 bit identifier
    - Algorithm Identifier – 8 bit identifier
    - Key Type – Traffic Encryption Key or Key Encryption Key
    - Physical ID, Common Key Reference (CKR) number, and Keyset number – Identifiers indicating storage locations.

    Along with the encrypted key data, this information is stored in a key record that includes a CRC over all of the fields to detect data corruption.
8. The Module denies access to plaintext secret and private keys contained within the module.
9. The Module provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the module.
10. The Module implements all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
11. The Module conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B requirements.

10 References and Definitions

The following standards are referred to in this Security Policy.

Table 16 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, *March 2019*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, December 2012*
[133r1]	*NIST Special Publication 800-133 Revision 1, Recommendation for Cryptographic Key Generation, July 2019*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[22r1a]	*National Institute of Standards and Technology, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April 2010*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*

Abbreviation	Full Specification Name
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*
[OTAR]	*Project 25 – Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures [TIA-102.AACA-A], September 2014*

Table 17 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CSP	Critical Security Parameter
DIA	Drop-In Algorithm
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECDSA	Elliptic Curve Digital Signature Algorithm
FW	Firmware
GCM	Galois/Counter Mode
IDK	Image Decryption Key
IV	Initialization Vector
KAT	Known Answer Test
KMF	Key Management Facility
KPK	Key Protection Key
KEK	Key Encryption Key
KVL	Key Variable Loader
OTAR	Over The Air Rekeying
PDA	Personal Digital Assistant
NDRNG	Non-Deterministic Random Number Generator
SA	Security Adapter
TEK	Traffic Encryption Key